данного подхода. Т. е., чем внимательнее пользователи при наборе текста, тем больше эффективность, кроме того, желательно, чтобы уровень внимательности пользователей был примерно одинаковым.

Главными недостатками данного подхода являются временные затраты для накопления учебных данных и их обработки, а также повышенные требования к используемой вычислительной технике.

Эти недостатки являются основными проблемами при применении данного подхода для решения задачи аутентификации пользователей компьютерных систем, поэтому можно сказать, что решение этих проблем – это одна из задач, которую необходимо решать в дальнейшем.

Литература: ***1.*** *Высоцкая Е. А., Давиденко А. Н. Анализ алгоритмов реализации выборочной политики безопасности в автоматизированных системах. Сборник научных трудов Института проблем моделирования в энергетике НАН Украины. Вып. 16, Киев, 2002 г., с. 124-130.* ***2.*** *Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. 452 с., ил.* ***3.*** *Гундарь К. Ю, Гундарь А. Ю., Янишевский Д. А. Защита информации в компьютерных системах. – К.: "Корнейчук", 2000. – 152 с., ил.* ***4.*** *Каллан Р. Основные концепции нейронных сетей.: Пер. с англ. – М.: Издательский дом "Вильямс", 2001. – 290с.* ***5.*** *Байдык Т. Н. Нейронные сети и задачи искусственного интеллекта. – К.: "Наукова думка", 2001. 265с.* ***6.*** *Архангельский В. И. и др. Нейронные сети в системах автоматизации. – К.: "Техника", 1999. – 364 с.* ***7.*** *neurnews.iu4.bmstu.ru/book/it/it898/stat1.htm/ Бондарев П. А. , Астафьев М. С. Распознавание отпечатков пальцев методами, использующими нейросети.* ***8.*** *nnet.chat.ru.nbp.html. Программа распознавания образов и прогноза.* ***9.*** *www.neuroproject.ru/index.htm/ Ward Systems Group, Inc. и компания НейроПроект* ***10.*** *www.neuroproject.ru/ Система определения настроения.* ***11.*** *www.neuroproject.ru/ Распознавание способа печати.* ***12.*** *Курош А. Г. Курс высшей алгебры. – М.: Государственное издательство физико-математической литературы, 1963. – 432с.*

УДК 681.3

МЕТОДИКИ ВИЗНАЧЕННЯ ВИХІДНИХ ДАНИХ ДЛЯ ОЦІНКИ ЗАЛИШКОВИХ РИЗИКІВ У ЛОМ

В'ячеслав Василенко, Микола Будько
Відкрите акціонерне товариство "КП ОТІ"

Анотація: **Пропонуються методики оцінки залишкових ризиків при забезпеченні конфіденційності, цілісності та доступності інформаційних об'єктів автоматизованих систем.**
Summary: **It is offered methods for the tasks of estimation of remaining risks at providing of confidentiality, integrity and availability of information's holding object of the automated systems.**
Ключові слова: **Інформація, конфіденційність, доступність, цілісність, вихідні дані.**

Вступ

Методики оцінки основних показників захищеності інформації в локальних обчислювальних мережах (ЛОМ) з достатньою глибиною розглянуті в [1, 2]. Але порядок визначення значень змінних (вихідних даних) у формульних виразах для оцінки величин відповідних залишкових ризиків в [1, 2] не наведено. У даній статті пропонуються підходи до їх визначення. Попередньо відзначимо, що чисельні значення змінних у наведених в [1, 2] виразах показників захищеності інформації [3 – 5] (ймовірностей порушення тієї чи іншої властивості захищеності інформації) можуть бути або розраховані (більшість з них), якщо відомі їх складові, чи закони розподілу відповідних ймовірностей, або визначені методом експертних оцінок. В останньому випадку ці показники потребують уточнення чи корегування службою захисту інформації відповідної організації, виходячи з досвіду експлуатації чи застосування системи захисту інформації ЛОМ, з наступною корекцією "Планів захисту інформації ЛОМ", заходів із захисту, складу та можливостей засобів захисту тощо.

У даній статті в більшості випадків розподіл імовірностей подій, пов'язаних зі спробами несанкціонованого доступу до інформаційних ресурсів, уважається рівномірним. Це пов'язано з тим, що, по–перше, такий закон розподілу є найскладнішим для функціонування систем захисту, а по друге, з відсутністю підстав для використання математичних апаратів інших законів розподілу. У разі можливості визначення параметрів потоків випадкових величин потрібні значення ймовірностей визначені з використанням відповідного математичного апарату.

Нижче, з урахуванням попередніх зауважень, викладені методики для практичного визначення вихідних даних для розрахунку показників захищеності інформації ЛОМ.

І Методика визначення вихідних даних для розрахунку показників конфіденційності інформації ЛОМ

В [2] ймовірність порушення конфіденційності $q_{пк}$ визначено як

$$q_{пк} = q_{кзі}\cdot[1-(1-q_1)\cdot(1-q_{зв})\cdot(1-q_{ав1})\cdot(1-q_{кткм})],$$

де $q_1 = q_{уфд}\cdot q_{ад}\,[1-(1-q_{оод})\cdot(1-q_{ос})]$.

Тому, як вихідні дані для визначення показників конфіденційності інформації ЛОМ необхідно визначити ймовірності подолання порушником (відповідною загрозою) засобів:

1. криптографічного захисту $q_{кзі} = q_{зм}\cdot q_{зкп}\cdot q_{кн}$;
2. захисту від витоків інформації технічними каналами $q_{зв}$;
3. організаційного обмеження доступу $q_{оод}$;
4. охоронної сигналізації $q_{ос}$;
5. захисту інформації від впливів із телекомунікаційної мережі $q_{ф}$;
6. управління фізичним доступом $q_{уфд}$;
7. адміністрування доступом $q_{ад}$;
8. антивірусного захисту $q_{ав}$.

Виходячи з моделей загроз та порушника, будемо вважати ймовірність знання порушником мови документу $q_{зм} = 1$, та ймовірність наявності в нього засобів криптографічного перетворення, особливо в зв'язку із вимогами застосування в Україні засобів криптографічного захисту лише за алгоритмами по ГОСТ 28147–89, $q_{зкп} = 1$. Якщо в складі засобів ТЗІ не використовуються засоби криптографічного перетворення усієї критичної інформації, то величину ймовірності $q_{кн}$ знання (наявності в порушника) ключових наборів також слід уважати такою, що $q_{кн} = 1$.

Примітка. При використанні в складі засобів ТЗІ засобів криптографічного перетворення усієї критичної інформації, величину ймовірності того, що порушник має необхідні ключі для засобів криптографічного перетворення $q_{кн}$, виходячи з умови їх надійного приховування відповідними користувачами, слід визначати з урахуванням необхідності прямого перебору усіх можливих ключових наборів. Наприклад, якщо засобами криптографічного перетворення реалізується алгоритм, аналогічний алгоритму за ГОСТ 28147–89 з кількістю варіантів ключів $N_{кл}=2^{256}$, то закон розподілу цієї ймовірності можна вважати рівномірним, і ймовірність подолання засобів криптозахисту $P_{кзі}$ може бути прийнятою рівною $q_{кн} = N_{кл}^{-1} = 2^{-256}$. При цьому ймовірність порушення конфіденційності $q_{пк}$ слід уважати знехтувано малою, незалежно від застосування інших засобів забезпечення конфіденційності. *Але такий варіант побудови системи захисту може бути неефективним у разі необхідності працювати з критичною інформацією: вводити з клавіатури, відображати на екранах моніторів та таке інше, коли порушення конфіденційності може бути здійснено за рахунок витоків інформації технічними каналами*.

Захист інформації від її витоків технічними каналами в ЛОМ слід розглядати [6] як сукупність заходів та засобів захисту від наступних видів витоків:

електромагнітних (по каналам побічного електромагнітного випромінювання);

електричних (за рахунок нерівномірності споживання струму);

параметричних (паразитної генерації шляхом застосування спеціального "ВЧ – опромінювання", електромагнітне поле якого взаємодіє з елементами ЗОТ і модулюється інформаційним сигналом);

при передачі інформації мережними кабелями (витік через мережні кабелі, особливо в разі розташування елементів ЛОМ у різних приміщеннях) з використанням індукційного перехоплення інформації; за опублікованими даними сучасні індукційні датчики здатні знімати інформацію не тільки з ізольованих кабелів, але й з кабелів, захищених подвійною бронею зі сталевої стрічки й сталевого дроту.

Зрозуміло, що ймовірність подолання порушником (відповідною загрозою) засобів захисту від витоків інформації технічними каналами $q_{зв}$ слід розглядати як імовірність складної події, яка полягає в наявності витоків тим чи іншим технічним каналом та в подоланні засобів захисту кожного із цих видів витоків.

Позначимо ймовірності наявності витоків електромагнітним, електричним, параметричним каналами та через мережні кабелі через $P_{емв}$, $P_{ев}$, $P_{пв}$ та $P_{мк}$ відповідно, а *умовні ймовірності* подолання засобів захисту кожного із цих видів витоків (при умові наявності відповідних витоків) – через $q_{емв}$, $q_{ев}$, $q_{пв}$, $q_{мк}$. Тоді

$$q_{зв} = P_{емв}\cdot q_{емв} + P_{ев}\cdot q_{ев} + P_{пв}\cdot q_{пв} + P_{мк}\cdot q_{мк}.$$

Методику розрахунку ймовірностей подолання засобів захисту кожного із цих видів витоків розглянемо на прикладі методики розрахунку ймовірностей подолання засобів захисту від електромагнітних витоків.

І. Перш за все, необхідно визначити ймовірності наявності кожного із видів витоків інформації ЛОМ. Це здійснюється за результатами обстеження приміщень та ЛОМ підприємства (їх засобів), під час якого встановлюються наявність і рівні відповідних витоків та здійснюється оцінка їх імовірностей.

На етапі попередньої оцінки ймовірності наявності кожного із видів витоку визначаються службою захисту інформації підприємства методом експертних оцінок.

Як приклад, з урахуванням особливостей відокремленої ЛОМ підприємства (живлення підприємства від окремої підстанції, живлення кожної із ЛОМ окремими фідерами, наявність мережних фільтрів в фідерах живлення, надійного заземлення, відсутність зв'язку з іншими ЛОМ тощо) методом експертних оцінок можуть бути встановлені наступні значення ймовірностей наявності:

електромагнітних (по каналам побічного електромагнітного випромінювання) витоків становить $P_{емв} = 0,8$;

електричних (за рахунок нерівномірності споживання струму) витоків становить $P_{ев} = 0,2$;

параметричних витоків дорівнює $P_{пв} = 0$.

витоків через мережні кабелі $P_{мк} = 0$.

Увага! При визначенні величин даних імовірностей слід дотримуватися нормуючої умови:

$$P_{емв} + P_{ев} + P_{пв} + P_{мк} = 1.$$

II. По друге, визначити ***умовні ймовірності*** подолання порушником засобів захисту по кожному із видів витоків – $q_{емв}$, $q_{ев}$, $q_{пв}$, $q_{мк}$.

Наведені нижче міркування щодо визначення умовних імовірностей подолання порушником засобів захисту для визначеності прив'язані до засобів захисту від витоків по каналам побічного електромагнітного випромінювання, хоча, зрозуміло, цей підхід може бути застосованим і до засобів захисту від витоків і іншими технічними каналами витоку з урахуванням їх певних особливостей.

Оскільки умовою захисту інформації є запобігання прийманню порушником без викривлень такої частки інформаційного об'єкту, яка є достатньою для сприйняття (розуміння) ним змісту даного інформаційного об'єкту (наприклад, повідомлення чи частки тексту), то не важко помітити, що така задача є класичною задачею визначення ймовірності приймання порушником сигналів в умовах впливу шумів (завад). З цієї задачі витікає й методика визначення необхідних вихідних даних – умовних імовірностей подолання порушником засобів захисту по кожному із видів витоків – $q_{емв}$, $q_{ев}$, $q_{пв}$, $q_{мк}$.

При цьому слід враховувати, що основними засобами захисту конфіденційності інформації є засоби зниження в точці приймання співвідношення сигнал/шум (засоби екранування приміщень, де розташовані елементи ЛОМ, чи власне елементів ЛОМ та генератори шумів, наприклад, типу "Волна – 4Р"). У цьому випадку при забезпеченні захисту від витоків інформації технічними каналами умовну ймовірність подолання порушником засобів захисту можна трактувати як імовірність правильного приймання порушником інформаційних сигналів, викривлених шумами $q_{емв} = 1 - P_{пом}$, де $P_{пом}$ – ймовірність викривлення в одному біті (ймовірність помилки).

Відомо [6], що ймовірність викривлення в одному біті (ймовірність помилки) $P_{пом}$ є функцією співвідношення сигнал/шум h^2 (див. рис. 1 [7, 8]):

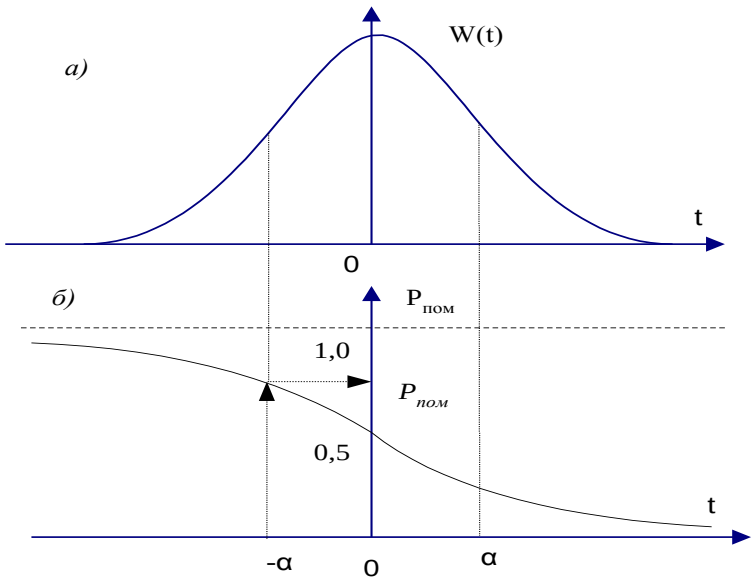

Рисунок 1 – До розрахунку ймовірності викривлення символів: *а)* центрована нормована щільність нормального закону імовірностей, *б)* ймовірність викривлення символу

$$P_{пом} = 1 - \Phi(\alpha),$$

де $\alpha = \sqrt{h^2/2}$, а $\Phi(\alpha) = 1/\sqrt{2\pi}\int_{-\infty}^{\alpha} e^{-t^2/2}dt$ – функція Лапласа (інтеграл імовірності помилки). Для обчислення цієї функції слід скористатися наступними відомими співвідношеннями. Для випадку $P_{пом} \le 0{,}5$:

$$\Phi(\alpha) = 1/\sqrt{2\pi}\int_{-\infty}^{\alpha} e^{-t^2/2}dt = 1/\sqrt{2\pi}\int_{-\infty}^{0} e^{-t^2/2}dt + 1/\sqrt{2\pi}\int_{0}^{\alpha} e^{-t^2/2}dt = 0{,}5 + 1/\sqrt{2\pi}\int_{0}^{\alpha} e^{-t^2/2}dt,$$

де $\Phi_0 = 1/\sqrt{2\pi}\int_{0}^{\alpha} e^{-t^2/2}dt$ – функція Лапласа-Гауса, яка є табульованою [7, 8]. Для даного випадку й достатньо великих значень цього співвідношення ($h^2 \ge 3$) вираз для розрахунку цієї ймовірності може бути наданим у вигляді [6]:

$$P_{пом} = 0{,}5\exp(-\alpha^2 h^2/2),$$

де h^2 – співвідношення сигнал/шум, $h^2 = P_c/P_ш$, P_c – потужність сигналу (в даному випадку – електромагнітного витоку) у діапазоні (в смузі) частот відповідного джерела витоку інформації (екрани, клавіатура, магнітні диски та таке інше), $P_ш$ – потужність адитивної суміші спеціальних шумів (шумів, які в даному випадку створюються спеціальними генераторами для маскування витоку сигналів), природних, індустріальних та інших шумів, α^2 – коефіцієнт, який залежить від виду модуляції сигналу (α^2=0,5 для амплітудної модуляції, сигналів типу відеосигнал, що є притаманними локальним обчислювальним мережам).

Для випадку маскування сигналів (запобігання витоку інформації технічними каналами) з урахуванням природної надлишковості мови, яка перевищує 50%, величину $P_{пом}$ за рахунок застосування генераторів шуму відповідної потужності чи за рахунок застосування засобів екранування приміщень або окремих елементів ЛОМ необхідно забезпечувати на рівні, який значно перевищує 0,5. Тоді (див. рис. 1):

$$\Phi(\alpha) = 1/\sqrt{2\pi}\int_{-\infty}^{\alpha} e^{-t^2/2}dt = 1/\sqrt{2\pi}\int_{-\infty}^{0} e^{-t^2/2}dt - 1/\sqrt{2\pi}\int_{0}^{-\alpha} e^{-t^2/2}dt =$$

$$= 0{,}5 + 1/\sqrt{2\pi}\int_{0}^{\alpha} e^{-t^2/2}dt.$$

$$P_{пом} = 0{,}5 + 1/\sqrt{2\pi}\int_{0}^{\alpha} e^{-t^2/2}dt, \quad (1)$$

$$\boldsymbol{q_{емв}} = 1 - P_{пом} = 0{,}5 - 1/\sqrt{2\pi}\int_{0}^{\alpha} e^{-t^2/2}dt, \quad (2)$$

причому при $\boldsymbol{P_{пом} \ge 0{,}5}$ **значення** h^2 у виразі $\alpha = \sqrt{h^2/2}$ повинно відображати співвідношення потужностей не сигналу і шуму, а навпаки, – **співвідношення потужностей шуму і сигналу**.

Вираз (1) слід і доцільно використовувати при $P_{пом} \le 0{,}997$ ($h^2 \le 3$), коли можна скористатися таблицями інтегралу Гауса. Неважко зрозуміти, що для даного випадку й достатньо великих значень цього співвідношення ($h^2 \ge 3$, $P_{пом} \ge 0{,}997$) вираз (1) для розрахунку останньої ймовірності може бути наданим у вигляді:

$$P_{пом} = 1 - 0{,}5\exp(-\alpha^2/4).$$

Отже, для випадку застосування генераторів маскуючих шумів і $P_{пом} \ge 0{,}5$; $h^2 \ge 3$

$$q_{емв} = 0{,}5\exp(-h^2/4). \quad (3)$$

Зауважимо, що оскільки генератори шуму та джерела витоків інформації по відношенню до засобів їх перехоплення (приймання) розташовані практично в одному місці (враховуючи, що відстань від точки приймання витоків до джерела витоків практично дорівнює відстані від точки приймання витоків до генератора), то співвідношення сигнал/шум в точці приймання є близьким до ***співвідношення сигнал/шум в точці, розташованій в безпосередній близькості до джерела витоків***.

Визначення величин $\boldsymbol{P_c}$ – потужності сигналу (в даному випадку – електромагнітного витоку) в діапазоні (в смузі) частот відповідного джерела витоку інформації (системні блоки, монітори, клавіатура,

магнітні диски та таке інше) та $P_ш$ – потужності адитивної суміші спеціальних шумів (шумів, які в даному випадку створюються спеціальними генераторами для маскування витоку сигналів), природних, індустріальних та інших шумів, а відтак – і співвідношення h^2 **здійснюється за результатами обстеження приміщень та елементів ЛОМ підприємства.**

Захист інформації від електричних витоків (за рахунок нерівномірності споживання струму), паразитної генерації та від витоків через мережні кабелі з використанням індукційного перехоплення інформації тощо, слід забезпечувати спеціальними елементами захисту інформації ЛОМ від витоку технічними каналами та спеціального впливу на неї (мережні та інші фільтри, надійне заземлення та т. ін.) Склад цих засобів, їх компонентів, механізмів, функцій та їх необхідні характеристики (коефіцієнти ослаблення сигналів витоку) визначаються на підставі обстеження відповідних джерел витоку інформації з урахуванням вимог плану ТЗІ та політики безпеки організації, як складової плану ТЗІ.

Методика визначення умовної ймовірності подолання порушником засобів захисту від електричних витоків $q_{ев}$, паразитної генерації $q_{пг}$, витоків через мережні кабелі з використанням індукційного перехоплення інформації $q_{мк}$ та відповідних вихідних даних не відрізняється від вище наведеної методики щодо визначення умовної ймовірності подолання порушником засобів захисту від електромагнітних витоків

III. Визначення, нарешті, шуканої ймовірності подолання порушником засобів захисту від порушення конфіденційності інформації за рахунок приймання витоків інформації технічними каналами:

$$q_{зв} = P_{емв} \cdot q_{емв} + P_{ев} \cdot q_{ев} + P_{пв} \cdot q_{пв} + P_{мк} \cdot \cdot q_{мк}.$$

Приклади. Визначимо ймовірності подолання порушником засобів захисту від порушення конфіденційності інформації за рахунок приймання витоків інформації технічними каналами для умов визначених на підставі обстежень співвідношень **шум/сигнал** h^2**.**

У табл. 1 наведено деякі проміжні результати та результати визначення шуканої ймовірності для значень h^2 = (0,54; 1,41; 3,24; 22). В останньому рядку таблиці наведено результати з використанням виразу (4).

Таблиця 1

h^2	$h^2/2$	$\Phi_0^{-1} = \alpha = \sqrt{h^2/2}$	Φ_0	$P_{пом}$	$q_{зв}$
0,54	0,27	0,52	0,2	0,7	0,3
1,41	0,706	0,84	0,3	0,8	0,2
3,24	1,64	1,28	0,4	0,9	0,2
22	11	–	–	0,998	0,002

Звернемо увагу на те, що значення співвідношення сигнал/шум на виході відповідних засобів захисту дорівнює практично коефіцієнту ослаблення сигналів витоку даного засобу.

Імовірності подолання порушником (відповідною віддаленою загрозою) засобів фільтрації зовнішніх (віддалених) загроз конфіденційності із телекомунікаційних мережа $q_{кткм}$ визначаються характеристиками засобів та протоколів внутрішньо та зовнішньо мережного обміну на транспортному, мережному та канальному рівнях семирівневої моделі взаємодії відкритих систем OSI.

Імовірність подолання засобів захисту інформації від несанкціонованого доступу в [*2*] *визначено як*

$$q_1 = q_{уд} \cdot [1 - (1 - q_{ood}) \cdot (1 - q_{oc}) (1 - q_ф)],$$

де величина $q_{уд}$ –ймовірність подолання засобів управління доступом, така, що $q_{уд} = q_{уфд} \cdot q_{ад}$.

Величина ймовірності подолання засобів управління фізичним доступом $q_{уфд}$ визначається можливостями системи автоматичної автентифікації з використанням носіїв Pin–кодів. Величина ймовірності подолання засобів управління фізичним доступом визначається кількістю символів в Pin–коді (довжиною Pin–коду) та кількістю символів додаткової інформації для автентифікації користувача n

$$q_{уфд} = 2^{-8n}.$$

При використанні носіїв Pin–кодів типу безконтактних ідентифікатор EM – 05 (чи інших, наприклад, карток контролю санкціонованого доступу EM – 4102, безконтактних ідентифікаторів Touch Memory DS 1990, Touch Memory DS 1991) $q_{уфд} = 2^{-k}$, де k – довжина коду, використаного для розміщення ідентифікаційної інформації (наприклад, для Touch Memory DS 1990 з довжиною унікального Pin–коду в 8 символів (байтів) $q_{уфд} = 2^{-64}$, при використанні носіїв Pin–кодів типу Touch Memory DS 1991 з довжиною унікального Pin–коду в 8 символів та трьома областями пам'яті (ідентифікатор – 8 байтів, пароль – 8 байтів, області Secure – 48 байти $q_{уфд} = 2^{-544}$).

Величина ймовірності $q_{ад}$ подолання засобів адміністрування доступом з використанням механізмів базового та прикладного програмного забезпечення визначається можливостями системи автентифікації з використанням паролів відповідних користувачів. Величину цієї ймовірності можна визначити через

кількість символів у паролі (довжину паролю) n користувача

$$q_{ад} = 2^{-8n}.$$

Величину q_{ood} – ймовірності подолання засобів організаційного обмеження доступу (ймовірність недотримання порушниками, у тому числі персоналом відповідних підрозділів, у яких використовуються ЛОМ, посадових інструкцій, наказів та розпоряджень керівництва щодо забезпечення безпеки інформації тощо) можна визначити методом експертних оцінок і прийняти, наприклад, на рівні $q_{ood} \approx 10^{-3}$.

Величина q_{oc} – ймовірності подолання засобів охоронної сигналізації визначається їх наявністю у відповідних підрозділах, кількістю рубежів виявлення, паспортними даними відповідних засобів виявлення (кутові та дальностні параметри діаграм направленості) та умовами їх застосування.

Імовірності подолання порушником (відповідною загрозою) засобів антивірусного захисту $q_{ав}$ можна визначити, знаючи, приміром, співвідношення між кількістю вірусів, занесених у базу засобів антивірусного захисту та загальною кількістю існуючих, точніше відомих на час оцінки, вірусів. Наприклад, якщо кількість вірусів, занесених у базу засобів антивірусного захисту, дорівнює $N_{вз}$, а загальна кількість відомих вірусів – $N_{вв}$, то величину $q_{ав}$ можна визначити із виразу

$$q_{ав} = 1 - N_{вз}/ N_{вв}.$$

II Методика визначення вихідних даних для розрахунку показників цілісності інформації ЛОМ

Нагадаємо, що в [2] ймовірність порушення цілісності $q_{пц}$ визначено як

$$q_{пц} = q_{кц} \cdot [1-(1-q_1)\cdot(1-q_{св})\cdot(1-q_{ав})].$$

У цьому виразі величина ймовірності q_1 та $q_{ав}$ визначається за наведеними вище рекомендаціями.

Величина ймовірності $q_{кц}$ подолання засобів контролю цілісності інформації (в разі їх наявності, інсталяції (установці) та застосуванні) визначається заданою адміністратором безпеки відповідного вузла довжиною ключа перетворення чи, відповідно, ознаки цілісності. Величину цієї ймовірності можна визначити, як і раніше, через кількість символів у ключовому наборі (довжину ключа) чи через кількість символів в ознаці цілісності

$$q_{кц} = 2^{-8n1},$$

де n1 – кількість символів у ключовому наборі (довжина ключа), який використовується при формуванні та контролі ознак цілісності.

Захист інформації від спеціального впливу технічними каналами, згідно з моделлю загроз, зводиться до захисту від електромагнітного впливу і може досягатися використанням засобів екранування приміщень чи (можливо – а також) екранованих засобів оброблення та передавання інформації, а також застосуванням засобів контролю та поновлення цілісності інформації.

Задача визначення ймовірності $q_{св}$ подолання засобів захисту від спеціального впливу на інформацію технічними каналами є, по суті, зворотною відносно задачі визначення ймовірності подолання засобів захисту від витоків інформації технічними каналами і зводиться до визначення ймовірності викривлення символів відповідного інформаційного об'єкту:

$$q_{св} = P_{пом},$$

де $P_{пом}$ – ймовірність викривлення (помилки) на символ (біт) інформації, яку потрібно захистити від спеціального впливу.

Звідсіля *після обстеження засобів обчислювальної техніки* з метою визначення рівнів власних витоків (рівня сигналу) та рівня спеціальних впливів технічними каналами отримати шукане значення ймовірності подолання засобів захисту від спеціального впливу на інформацію технічними каналами – $q_{св}$.

Використовуючи раніше наведені вирази для розрахунку ймовірності викривлення в одному біті (помилки) $P_{пом}$, а також зауваження щодо типу модуляції сигналів, отримаємо:

$$q_{св} = P_{пом} \geq 2\exp(-h^2/4), \qquad (5)$$

при $h^2 \geq 3$, або при $h^2 \leq 3$:

$$P_{пом} = 1 - \Phi(\alpha).$$

Таким чином,

$$q_{св} = P_{пом} = 1 - \Phi(\alpha) = 0{,}5 - \Phi_0, \qquad (6)$$

де h^2 – співвідношення сигнал/вплив (сигнал/шум) у точці розташування елементів ЛОМ, здатних реагувати на спеціальні впливи технічними каналами.

Зауваження. Для випадку оцінки ймовірності подолання порушником засобів забезпечення цілісності доцільніше скористатися тим, що співвідношення енергетик сигнал/вплив може бути замінено на співвідношення квадратів відповідних значень напруг, тобто визначатися не як співвідношення потужностей (енергетик) відповідних електромагнітних полів у точці розташування елементів ЛОМ, а як

співвідношення квадрату значення напруги сигналу, наведеного за рахунок спеціальних впливів на найдовшому із провідників елементу ЛОМ, у якому циркулюють інформаційні сигнали, до квадрату значення напруги логічної одиниці в тому ж із провідників:

$$h^2 = U_{ло}^2 / U_{св}^2,$$

де для відповідних ланцюгів з найдовшим із провідників елементу ЛОМ: $U_{ло}$ – рівень напруги логічної одиниці, $U_{св}$ – рівень напруги наводок за рахунок спеціальних впливів.

Приклади. Визначимо ймовірності подолання порушником засобів захисту від порушення цілісності інформації за рахунок спеціальних впливів на інформацію технічними каналами для умов, визначених на підставі обстежень співвідношень сигнал/шум h^2.

У табл. 2 наведено деякі проміжні результати та результати визначення шуканої ймовірності для значень h^2 = (0,54; 1,41; 22; 60, 120). У перших трьох рядках таблиці наведено результати з використанням виразу (5), а в останніх двох – з використанням виразу (6).

Таблиця 2

h^2	$\Phi_0^{-1} = \alpha = \sqrt{h^2/2}$	Φ_0	$P_{пом} = q_{св}$
120	–	–	$0{,}9\cdot10^{-15}$
60	–	–	$0{,}3\cdot10^{-8}$
22	–	–	0,002
1,41	0,84	0,3	0,2
0,54	0,52	0,2	0,3

III Методика визначення вихідних даних для розрахунку показників доступності інформації ЛОМ

Виходячи із визначення доступності як функціональної властивості захищеності інформаційних об'єктів, будемо визначати як її кількісні характеристики імовірність порушення доступності $q_{пд}$ та час затримки доставки інформаційних об'єктів (кадрів, пакетів, повідомлень тощо) від їх джерела до отримувача.

3.1 Визначення ймовірності порушення доступності

Нагадаємо, що в [2] ймовірність порушення доступності $q_{пд}$ визначено як:

$$q_{пд} = 1 - (1 - q_{з})\cdot(1 - q_{пц}).$$

У цьому виразі вимоги щодо вихідних даних для визначення величини $q_{пц}$ визначено, в основному, у попередньому розділі, а величина

$$q_{пз} = 1 - p_{0i} = 1 - \exp\{-t_{вр}\cdot\lambda_з\}.$$

Для деякого спрощення задачі надалі будемо вважати ЛОМ відокремленою, тобто такою, що не має зв'язку з іншими ЛОМ, а також такою, що використовується протягом робочого часу користувачів. У цьому випадку змінні в останньому виразі можна визначати наступним чином:

величина $\lambda_з$ є результуючою інтенсивності загроз захищеному ресурсу ЛОМ

$$\lambda_з = \sum_{i=1}^{i=3} (\lambda_{шві} + \lambda_{шзі}\cdot q_ф)\cdot q_{ад} + \lambda_{сз} + \lambda,$$

де $\lambda_{шві}$ – інтенсивність штучних внутрішніх впливів (загроз) через засоби управління доступом.

Штучні внутрішні загрози, взагалі, складаються із навмисних та ненавмисних загроз з боку користувачів елементів ЛОМ, перш за все, користувачів ПЕОМ. Навмисними загрозами, враховуючи наявність досить організованого контролю з боку служби захисту інформації, адміністраторів мереж та керівництва підрозділів, можна знехтувати. Інтенсивність невмисних (помилкових) дій користувачів елементів ЛОМ визначається кількістю користувачів (кількістю ПЕОМ даної ЛОМ), ступенем їх комп'ютерної підготовки та втомленості. Для початкових розрахунків будемо вважати, що з кожної ПЕОМ (кожен користувач) може допустити один помилковий запит протягом робочого дня. При кількості ПЕОМ у складі ЛОМ $n_к$ і тривалості робочого дня 8 год. 12 хв. = 29520 с будемо мати

$$\sum_{i=1}^{i=3} \lambda_{шві} \approx 3{,}39\cdot10^{-5}\cdot n_к \ 1/с,$$

де $\lambda_{шві}$ – інтенсивність штучних зовнішніх (спеціальних, зловмисних) впливів (загроз) технічними каналами через засоби їх блокування (в разі наявності зв'язку даної ЛОМ з іншими ЛОМ чи підключенні її до розподілених інформаційно – телекомунікаційних мереж. Для умов відокремленої ЛОМ $\lambda_{шзі} = 0$); $\lambda_{сз}$ – інтенсивність справжніх запитів, яка залежить від кількості ПЕОМ даної ЛОМ $n_к$, середньої кількості інформаційних об'єктів (задач), що потребують використання протягом робочого дня на кожній із ПЕОМ $n_{зк}$.

Для початкових розрахунків будемо вважати, що кожен з інформаційних об'єктів кожної із ПЕОМ використовується протягом робочого дня хоча б один раз. Тоді

$$\lambda_{сз} \approx 3{,}39 \cdot 10^{-5} \cdot n_к \cdot n_{зк} \text{ 1/с},$$

де $q_ф$ – ймовірність подолання засобів блокування (фільтрації) зовнішніх (спеціальних, зловмисних) впливів (загроз) технічними каналами (в разі наявності зв'язку даної ЛОМ з іншими ЛОМ чи підключенні її до розподілених інформаційно – телекомунікаційних мереж) визначається характеристиками їх засобів автентифікації, блокування, протоколів, proxy – серверів, засобів антивірусного захисту, правил безпеки (частковою політикою безпеки). Для умов відокремленої ЛОМ, як і вище $q_ф = 0$, і тоді:

$$\lambda_з = \sum_{i=1}^{i=3} \lambda_{шві} \cdot q_{ад} + \lambda_{сз} + \lambda,$$

де λ – інтенсивність природних впливів (загроз).

Під природними загрозами будемо розуміти впливи, пов'язані зі збоями в роботі обладнання елементів ЛОМ за рахунок електромагнітних впливів розрядів атмосферної електрики, відключення електромереж, іскріння в контактах та контактних мережах авто– та електротранспорту, електромереж, іскріння під час електрозварювальних робіт, збоях та відмовах із-за недостатньої надійності елементної бази та т. ін. Для початкових розрахунків будемо вважати, що хоча б одна із таких подій трапляється протягом тижня хоча б один раз:

$$\lambda \approx 6{,}8 \cdot 10^{-6} \text{ 1/с},$$

де $q_{ад}$ – ймовірність подолання загрозами засобів управління доступом.

Ця ймовірність визначається за методикою, наведеною вище.

Таким чином, для початкових розрахунків можна вважати:

$$\lambda_з = \sum_{i=1}^{i=3} \lambda_{шві} \cdot q_{ад} + \lambda_{сз} + \lambda \approx 3{,}39 \cdot 10^{-5} \cdot n_к + 3{,}39 \cdot 10^{-5} \cdot n_к \cdot n_{зк} + 6{,}8 \cdot 10^{-6} =$$

$$\approx 3{,}39 \cdot 10^{-5} \cdot (n_к + n_к \cdot n_{зк} + 0{,}2) \text{ 1/с};$$

змінна $t_{вр}$ – оцінка (середнє значення) часу, що може бути наданим захищеному ресурсу для свого використання при заданій чи потрібній перепускній спроможності відповідного вузла ЛОМ (для інформаційних об'єктів це – контроль цілісності, при необхідності її поновлення – середній час виконання програмного засобу, читання чи запису та корегування інформації та все таке інше). У термінах теорії масового обслуговування ця змінна визначає інтенсивність обслуговування запитів коли $\mu = 1/ t_{вр}$. Для початкових розрахунків будемо вважати, що цей час визначається періодичністю контролю так, що T_{ki} дорівнює тривалості робочого дня, тоді тривалістю контролю ΔT_{ki} можна знехтувати. Якщо середня кількість задач, що реалізуються на кожній із ПЕОМ, є $n_{зк}$ та кожна із них виконується хоча б один раз протягом робочого дня, то

$$t_{вр} = 29520/ n_{зк} \text{ с}.$$

При таких умовах отримаємо початкове значення величин

$$q_{п3} = 1 - \exp\{-t_{вр} \cdot \lambda_з\} = 1 - \exp[-(n_к + n_к \cdot n_{зк} + 0{,}2) / n_{зк}],$$

$$q_{пд} = 1 - \exp[-(n_к + n_к \cdot n_{зк} + 0{,}2) / n_{зк}] \cdot (1 - q_{пц}),$$

де значення $q_{пц}$ обраховується за вище розглянутою методикою.

Значення реальних інтенсивностей впливів (інтенсивність справжніх запитів $\lambda_{сз}$, інтенсивність спеціальних впливів (загроз) по технічним каналам – $\lambda_{шзі}$, інтенсивність природних впливів (загроз) λ та результуюча інтенсивності загроз захищеному ресурсу можуть бути визначеними (оціненими) під час обстеження відповідних ЛОМ (дослідження інформаційних потоків), з досвіду експлуатації елементів ЛОМ чи визначеними методом експертних оцінок.

У разі використання невідокремлених ЛОМ імовірність подолання засобів блокування засобів генерації безперервних запитів, спроб підбору паролів та т. п. $q_ф$ визначається характеристиками їх засобів автентифікації, блокування, протоколів, proxy – серверів, засобів антивірусного захисту, правил безпеки (частковою політикою безпеки).

3.2 Визначення часу затримки доставки інформаційних об'єктів

При визначенні часу затримки доставки інформаційних об'єктів (кадрів, пакетів, повідомлень тощо) від джерела в складі однієї із ЛОМ до отримувача в складі другої ЛОМ (*при умові наявності зв'язку даної ЛОМ з іншими ЛОМ у розподіленій інформаційно – обчислювальній мережі підприємства чи з іншими розподіленими інформаційно – обчислювальними мережами)* врахуємо, що загальний час затримки доставки складається із затримок у доставці повідомлень на маршруті передачі в засобах управління зовнішньомережним та внутрішньомережним доступом, а також із затримки власне в середовищі передачі інформації розподіленої мережі (див. рис. 2).

1. Для визначення часу затримки доставки інформаційних об'єктів у засобах управління зовнішньомережним доступом до інформаційних ресурсів (фільтрації пакетів, блокування безперервних зовнішньомережних запитів, спроб підбору паролів та т. п.) у складі серверів доступу (чи маршрутизаторів,
міжмережних екранів, firewall'ів, брандмауерів, proxy – серверів тощо) будемо розглядати ці засоби як деяку систему масового обслуговування (СМО).

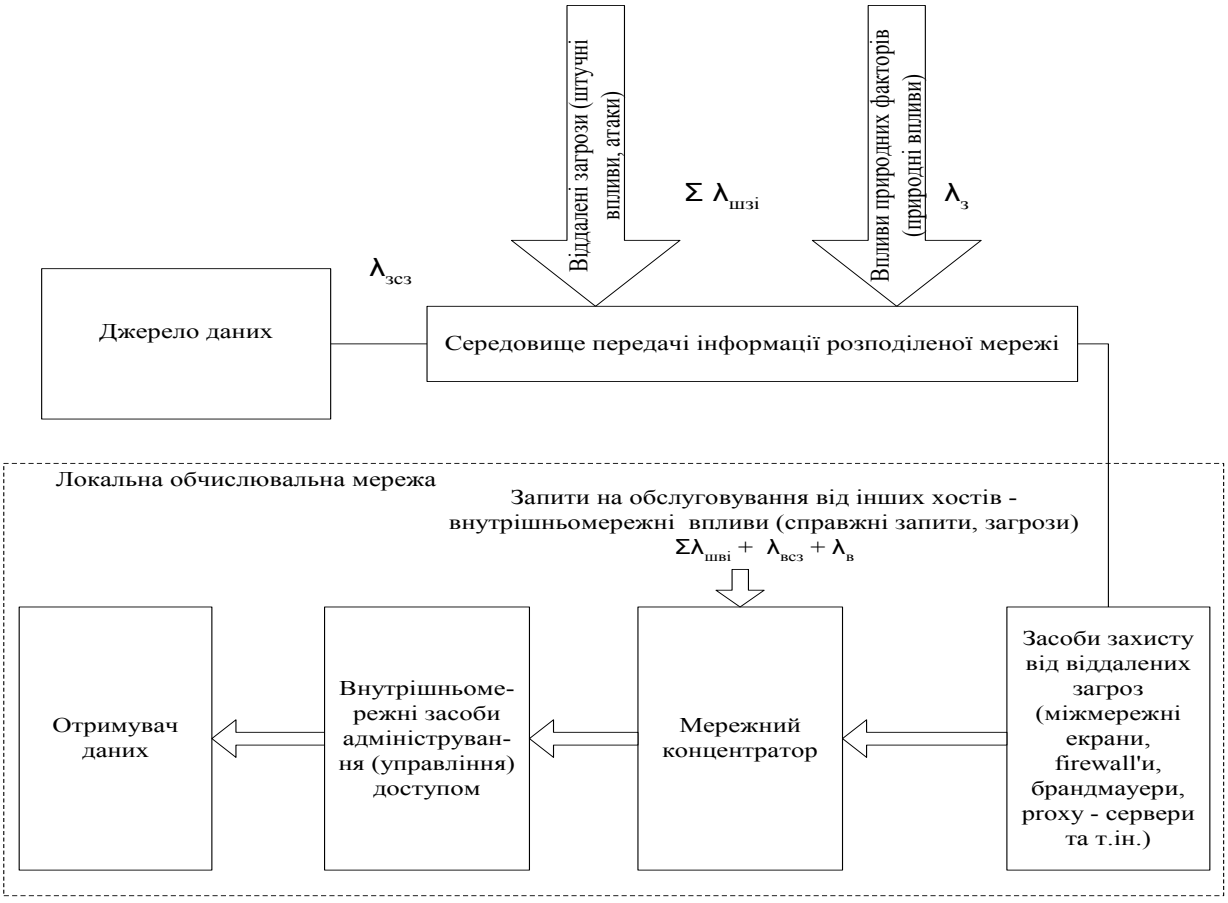

Рисунок 2 – Взаємодія засобів у процесі передачі даних (доставляння повідомлень)

У цій СМО вхідний потік зовнішніх (по відношенню до ЛОМ) запитів із інтенсивністю

$$\lambda_{зр} = \sum_{i=1}^{i=3} \lambda_{шзі} + \lambda_{зс} + \lambda_{з}$$

перетворюється в потік зовнішніх запитів (впливів) із інтенсивністю $\lambda_{зз}$

$$\lambda_{зз} = \sum_{i=1}^{i=3} \lambda_{шзі} \cdot q_{ф} + \lambda_{зс} + \lambda_{з};$$

де $\lambda_{зр}$ – інтенсивність результуючого потоку зовнішніх запитів на обслуговування засобами управління

зовнішньомережним доступом до інформаційних ресурсів.

Для даного випадку потік запитів слід розглядати як такий, що утворюється сукупністю з потоків усіх зовнішніх штучних загроз $\lambda_{шзі}$ (нагадаємо – i = 1, 2, 3, загрози конфіденційності, цілісності та доступності), зовнішніх справжніх запитів $\lambda_{зс}$ та зовнішніх природних впливів λ (інтенсивність яких залежить від співвідношенням сигнал/завада в середовищі передачі інформації розподіленої мережі); $q_ф$ – ймовірність подолання зовнішньомережними загрозами засобів управління зовнішньомережним доступом.

2. Для визначення часу затримки доставки інформаційних об'єктів у засобах внутрішньомережного адміністрування (управління) доступом до інформаційних ресурсів отримувача даних будемо розглядати їх також як СМО. На вхід даної СМО поступає потік запитів, який складається із потоку зовнішніх впливів з інтенсивністю $\lambda_{зз,}$ потоку внутрішніх штучних впливів (загроз) із інтенсивністю $\lambda_{шві}$, потоку внутрішніх справжніх запитів із інтенсивністю $\lambda_{всз}$ та потоку внутрішніх природних впливів $\lambda_в$ (інтенсивність яких також залежить від співвідношенням сигнал/завада в середовищі передачі інформації локальної мережі):

$$\lambda_{рз} = \sum_{i=1}^{i=3} (\lambda_{шві} + \lambda_{шзі} \cdot q_ф) + \lambda_{сз} + \lambda.$$

де $\lambda_{сз}$ – інтенсивність результуючого потоку справжніх запитів $\lambda_{сз} = \lambda_{зсз} + \lambda_{всз}$; λ – інтенсивність результуючого потоку природних запитів $\lambda = \lambda_з + \lambda_в$.

Внаслідок цієї взаємодії вхідний потік запитів з інтенсивністю $\lambda_{рз}$ перетворюється в потік впливів із інтенсивністю $\lambda_з$

$$\lambda_з = \sum_{i=1}^{i=3} (\lambda_{шві} + \lambda_{шзі} \cdot q_ф) \cdot q_{ад} + \lambda_{сз} + \lambda,$$

де $q_{ад}$ – ймовірність подолання результуючим потоком загроз засобів внутрішньомережного адміністрування (управління) доступом до інформаційних ресурсів.

Враховуючи характеристики віддалених загроз (перш за все загроз, спрямованих на досягнення відмов в обслуговуванні) першу зі СМО (засоби управління зовнішньомережним доступом до інформаційних ресурсів) можна розглядати, наприклад, як однофазну, одноканальну СМО з очікуванням. Для таких СМО відомими є вирази для обрахування математичного очікування тривалості початку обслуговування або, як уважають за краще говорити, середню тривалість очікування – час затримки повідомлення $\Delta t_{пф}$ в засобах фільтрації зовнішніх впливів (управління зовнішньомережним доступом):

$$\Delta t_{пф} = \rho^2 / (\lambda_{зр}(1-\rho)) = \lambda_{зр} t_{обс}^2 / (1-\lambda_{зр} t_{обс}),$$

де для визначеного типу СМО: $\rho = \lambda_{зр} / \mu$ – ймовірність відмови в обслуговуванні; μ – інтенсивність обслуговування запитів у СМО:

$$\mu = 1/t_{обс},$$

$t_{обс}$ – середній час оброблення (обслуговування) запитів у СМО.

Аналогічні міркування щодо другої зі СМО (засоби внутрішньомережного адміністрування (управління) доступом), середню тривалість очікування – час затримки повідомлення $\Delta t_{пад}$ в засобах адміністрування (управління) внутрішньомережним доступом:

$$\Delta t_{пад} = \rho^2 / (\lambda_з(1-\rho)) = \lambda_з t_{обсад}^2 / (1-\lambda_з t_{обсад}),$$

де $t_{обсад}$ – повідомлення $\Delta t_п$ в засобах фільтрації зовнішніх впливів (управління зовнішньомережним доступом) та в засобах адміністрування (управління) внутрішньомережним доступом

$$\Delta t_п = \Delta t_{пф} + \Delta t_{пад}.$$

3. Визначення часу затримки доставки інформаційних об'єктів у засобах середовища передачі інформації розподіленої мережі. Порядок визначення величин затримки для протоколів обміну, які реалізують способи обміну із вирішуючим зворотним зв'язком ($\Delta t_{пВЗЗ}$) чи із застосуванням завадостійких корегуючих кодів ($\Delta t_{пЗКК}$) визначається за окремою методикою і в межах даної статті не наводиться.

Таким чином, загальна величина часу $\Delta t_{здп}$ затримки доставки інформаційних об'єктів

$$\Delta t_{здп} = \Delta t_{пВЗЗ} + \Delta t_{пф} + \Delta t_{пад}$$

у разі застосування протоколів обміну із вирішуючим зворотним зв'язком чи

$$\Delta t_{здп} = \Delta t_{пЗКК} + \Delta t_{пф} + \Delta t_{пад}$$

у разі використання протоколів обміну із застосуванням завадостійких корегуючих кодів.

Примітка 4. Усі невизначені змінні у виразах, наведених для розрахунку запропонованих показників захищеності інформації (ймовірностей порушення тієї чи іншої властивості захищеності інформації), можуть бути розраховані, якщо відомі чи їх складові, чи закони розподілу відповідних імовірностей. У багатьох випадках можна вважати розподіл імовірностей таких подій рівномірним, принаймні, як найскладніший для функціонування систем захисту. В інших випадках для розрахунку ймовірностей можна використати параметри потоків відповідних випадкових величин. Оскільки детальний розгляд цього питання виходить за межі методики, обмежимося лише прикладом визначення ймовірностей, коли йдеться про необхідність прямого перебору, чи то ключових наборів (для засобів криптозахисту, контролю цілісності, та інше), чи то паролів (для засобів управління доступом та тому подібне), коли закони розподілу можна вважати рівномірним. Якщо відома, наприклад, кількість варіантів ключів засобів криптографічного захисту інформації $N_{кл} = 2^{256}$, тоді ймовірність $P_{кзі}$ може бути прийнятою рівною $P_{кзі} = N_{кл}^{-1} = 2^{-256}$.

Висновки

Запропонована методика дозволяє отримати вирази для визначення показників захищеності інформації по кожній з функціональних послуг захисту від можливих загроз у вигляді залишкового ризику – ймовірності порушення захисту від загроз відповідного типу – та побудувати загальну модель системи захисту в частині забезпечення необхідних властивостей захищеності й, за умовою оптимізації параметрів та характеристик відповідно до [5], може бути використаною для проектування ефективних систем технічного захисту інформації взагалі та їх складових зокрема.

Література: ***1.*** *Будько М. М. Визначення залишкового ризику при оцінці захищеності інформації в інформаційно – обчислювальних системах. К. НТУУ "КПІ" //Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Випуск 8// 2004, с. 20 – 26.* ***2.*** *Матов О. Я., Василенко В. С., Будько М. М. Визначення залишкового ризику при оцінці захищеності інформації в інформаційно – телекомунікаційних системах. // К.: Реєстрація, зберігання і обробка даних, 2004, Т. 6, № 2, с. 62 – 74.* ***3.*** *Нормативний документ. Системи технічного захисту інформації "Загальні положення про захист інформації в комп'ютерних системах від несанкціонованого доступу" (НД ТЗІ 1.1 – 002 – 99).* ***4****. Нормативний документ. Системи технічного захисту інформації "Критерії оцінки захищеності інформації в комп'ютерних системах від НСД" (НД ТЗІ 2.5 – 004 – 99).* ***5****. Нормативний документ Системи технічного захисту інформації "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу" (НД ТЗІ 2.5. – 005 – 99).* ***6.*** *Бунин С. Г., Войтер А. П. Вычислительные сети с пакетной радиосвязью. – К.: Техніка, 1989. – 223 с.* ***7****. Бронштейн И. Н., Семендяев К. А. Справочник по математике для инженеров и учащихся ВТУЗов.–М.: Наука, 1981.* ***8.*** *Абенгауз Г. Г. и. др. Справочник по вероятностным расчетам. – М. Воениздат МО, 1970.*